



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/982,711	10/18/2001	Taizo Shirai	09812.0590-00000	8666

22852 7590 04/18/2007

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP

901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER

KHOSHNOODI, NADIA

ART UNIT

PAPER NUMBER

2137

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
2 MONTHS	04/18/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.



09982711 UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

RECEIVED

APR 18 2007

Technology Center 2100

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

Application Number: 09/982,711
Filing Date: October 18, 2001
Appellant(s): SHIRAI ET AL.

Arthur A. Smith
Reg. No. 56,877
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 12/20/2006 appealing from the Final Office
Action mailed 4/26/2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct. The proposed amendment filed with the Appeal brief has been entered. The Amendment cancels claims 2-4, 7, 9-11, 14, 18-20, 23, 25-27, and 30.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is substantially correct. However, due to the fact that Appellant has cancelled claims 2-4, 7, 9-11, 14, 18-20, 23, 25-27, and 30, the changes are as follows:

Claims 1, 5, 8, 12, 15-17, 21, 24, 28, and 31-32 stand rejected under 35 U.S.C. 103(a) as being unpatentable over *Hazard* (U.S. Patent No. 6,658,566) in view of *Sudia* (Published U.S. Patent Application No. 2005/0114666).

Claims 6, 13, 22, and 29 stand rejected under 35 U.S.C. 103(a) as being unpatentable over *Hazard* (U.S. Patent No. 6,658,566) in view of *Sudia* (Published U.S. Patent Application No. 2005/0114666), and further in view of *Dilkie* (U.S. Patent No. 6,341,164).

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,658,566	Hazard	09-1998 (PCT Pub. Date)
2005/0114666	Sudia et al.	05-2005
6,341,164	Dilkie et al.	01-2002

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

IV. Claims 1, 5, 8, 15-17, 21, 24, 28, and 31-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hazard, United States Patent No. 6,658,566 and further in view of Sudia et al., United States Pub. No. 2005/0114666. As per claims 1 and 17:

Hazard substantially teaches an information recording device and method for executing processing which stores data to a memory having a data storage area consisting of a plurality of blocks, each of the blocks consists of M sectors from a first

sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number (col. 5, lines 15-39 and fig. 3), said information recording device comprising a cryptosystem unit which selectively uses different encryption keys for each sectors from the first sector to the M-th sector to execute encryption processing and the cryptosystem unit executes encryption processing on data to be stored in each of the sectors (col. 5, lines 1-14 and fig. 2).

Not explicitly disclosed is a revocation list having revocation information and a block permission table for accessing a permission table that describes memory access control information. However, Sudia et al. teach a table that contains information regarding all of the possible privileges a user may have (par. 237). Furthermore, Sudia et al. teach maintaining a revocation list in order to indicate that a privilege is no longer valid (par. 244-246). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hazard et al. to have revocation information and a block permission table for accessing a permission table that describes memory access control information. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Sudia et al. suggest that incorporating a permissions table and revocation information add to the security of the system in order to determine who may or may not gain access to specific resources at the time the user is attempting to do so in par. 237 and par. 245.

Also not explicitly disclosed is checking the integrity of the revocation list and checking the integrity of the block permission table. However, Sudia et al. teach that it

Art Unit: 2137

is important to check the integrity of the information in the tables that ultimately allow users' access to resources in order to ensure that the permissions/revocation list is being enforced in such a way that a user exceeds their permissions/resources that they should be able to access (par. 219, par. 237, and par. 244-245). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hazard et al. to have an integrity unit in order to ensure the integrity of the revocation list and block permission table. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Sudia et al. suggest that the permissions and revocation information may be included in the hashed value in order to ensure the validity of the data and that the data has not been improperly modified in par. 219, par. 237, and par. 244-245.

As per claims 5 and 21:

Hazard and Sudia et al. substantially teach an information recording device and method of claim 1. Furthermore, Hazard teaches the information recording device and method wherein, in said cryptosystem unit, the encryption processing for the first sector to the M-th sector is executed as single-DES encryption processing using different encryption keys for the sectors (col. 4, lines 32-46).

As per claims 8 and 24:

Hazard substantially teaches the information recording device and method for executing processing which reads data from a memory having a data storage area consisting of a plurality of blocks, each of which consists of the first sector to the M-th

sector which each have a predetermined data capacity, where M represents a natural number (col. 5, lines 15-39 and fig. 3), said information playback device comprising a cryptosystem unit which selectively uses different decryption keys for the first sector to M-th sector to execute decryption processing and which executes decryption processing on data stored in each of the sectors (col. 4, lines 32-46, col. 5, lines 1-14, and fig. 2). Not explicitly disclosed is a revocation list having revocation information and a block permission table for accessing a permission table that describes memory access control information. However, Sudia et al. teach a table that contains information regarding all of the possible privileges a user may have (par. 237). Furthermore, Sudia et al. teach maintaining a revocation list in order to indicate that a privilege is no longer valid (par. 244-246). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hazard et al. to have revocation information and a block permission table for accessing a permission table that describes memory access control information. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Sudia et al. suggest that incorporating a permissions table and revocation information add to the security of the system in order to determine who may or may not gain access to specific resources at the time the user is attempting to do so in par. 237 and par. 245.

Also not explicitly disclosed is checking the integrity of the revocation list and checking the integrity of the block permission table. However, Sudia et al. teach that it is important to check the integrity of the information in the tables that ultimately allow

users' access to resources in order to ensure that the permissions/revocation list is being enforced in such a way that a user exceeds their permissions/resources that they should be able to access (par. 219, par. 237, and par. 244-245). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hazard et al. to have an integrity unit in order to ensure the integrity of the revocation list and block permission table. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Sudia et al. suggest that the permissions and revocation information may be included in the hashed value in order to ensure the validity of the data and that the data has not been improperly modified in par. 219, par. 237, and par. 244-245.

As per claims 12 and 28:

Hazard and Sudia et al. substantially teach an information recording device and method of claim 8. Furthermore, Hazard teaches an information playback device and method wherein, in said cryptosystem unit, the decryption processing for the first sector to the M-th sector is executed as single-DES decryption processing using different decryption keys for the sectors (col. 4, lines 32-46).

As per claim 15:

Hazard substantially teaches an information recording medium having a data storage area consisting of a plurality of blocks, each of which consists of the first sector to the M-th sector which each have a predetermined data capacity, where M represents a natural number (col. 5, lines 15-39 and fig. 3), wherein a plurality of different

cryptographic keys which are selectable for the sectors are stored as header information of data stored in said data storage area (col. 5, lines 35-39). Although the term "header information" is not specifically used, the information is stored in such a way that it is identical to that of header information. Not explicitly disclosed is a revocation list having revocation information and a block permission table for accessing a permission table that describes memory access control information. However, Sudia et al. teach a table that contains information regarding all of the possible privileges a user may have (par. 237). Furthermore, Sudia et al. teach maintaining a revocation list in order to indicate that a privilege is no longer valid (par. 244-246). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hazard et al. to have revocation information and a block permission table for accessing a permission table that describes memory access control information. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Sudia et al. suggest that incorporating a permissions table and revocation information add to the security of the system in order to determine who may or may not gain access to specific resources at the time the user is attempting to do so in par. 237 and par. 245.

Also not explicitly disclosed is checking the integrity of the revocation list and checking the integrity of the block permission table. However, Sudia et al. teach that it is important to check the integrity of the information in the tables that ultimately allow users' access to resources in order to ensure that the permissions/revocation list is

Art Unit: 2137

being enforced in such a way that a user exceeds their permissions/resources that they should be able to access (par. 219, par. 237, and par. 244-245). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hazard et al. to have an integrity unit in order to ensure the integrity of the revocation list and block permission table. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Sudia et al. suggest that the permissions and revocation information may be included in the hashed value in order to ensure the validity of the data and that the data has not been improperly modified in par. 219, par. 237, and par. 244-245.

As per claim 16:

Hazard and Sudia et al. substantially teach an information recording device and method of claim 15. Furthermore, Hazard teaches an information recording medium, wherein said plurality of different cryptographic keys are M different encryption keys corresponding to the M sectors (col. 5, lines 1-14 and fig. 2).

As per claim 31:

Hazard substantially teaches a program providing medium for providing a computer program which controls a computer system to execute processing which stores data in a memory having a data storage area consisting of a plurality of blocks, each of which consists of the first sector to the M-th sector which each have a predetermined data capacity, where M represents a natural number (col. 5, lines 15-39 and fig. 3), said computer program comprising a data-encrypting step in which

encryption processing on data to be stored in the sectors is executed by performing encryption using encryption keys selected for the first sector to the M-th sector (col. 5, lines 1-14 and fig. 2).

Not explicitly disclosed is a revocation list having revocation information and a block permission table for accessing a permission table that describes memory access control information. However, Sudia et al. teach a table that contains information regarding all of the possible privileges a user may have (par. 237). Furthermore, Sudia et al. teach maintaining a revocation list in order to indicate that a privilege is no longer valid (par. 244-246). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hazard et al. to have revocation information and a block permission table for accessing a permission table that describes memory access control information. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Sudia et al. suggest that incorporating a permissions table and revocation information add to the security of the system in order to determine who may or may not gain access to specific resources at the time the user is attempting to do so in par. 237 and par. 245.

Also not explicitly disclosed is checking the integrity of the revocation list and checking the integrity of the block permission table. However, Sudia et al. teach that it is important to check the integrity of the information in the tables that ultimately allow users' access to resources in order to ensure that the permissions/revocation list is being enforced in such a way that a user exceeds their permissions/resources that they

Art Unit: 2137

should be able to access (par. 219, par. 237, and par. 244-245). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hazard et al. to have an integrity unit in order to ensure the integrity of the revocation list and block permission table. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Sudia et al. suggest that the permissions and revocation information may be included in the hashed value in order to ensure the validity of the data and that the data has not been improperly modified in par. 219, par. 237, and par. 244-245.

As per claim 32:

Hazard substantially teaches program providing medium for providing a computer program which controls a computer system to execute processing which reads data from a memory having a data storage area consisting of a plurality of blocks, each of which consists of the first sector to the M-th sector which each have a predetermined data capacity, where M represents a natural number (col. 5, lines 15-39 and fig. 3), said computer program comprising a data-decrypting step in which decryption of data stored in each of the sectors is performed by executing decryption processing using decryption keys selected in accordance with the first sector to the M-th sector (col. 4, lines 32-46, col. 5, lines 1-14, and fig. 2).

Not explicitly disclosed is a revocation list having revocation information and a block permission table for accessing a permission table that describes memory access control information. However, Sudia et al. teach a table that contains information

Art Unit: 2137

regarding all of the possible privileges a user may have (par. 237). Furthermore, Sudia et al. teach maintaining a revocation list in order to indicate that a privilege is no longer valid (par. 244-246). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hazard et al. to have revocation information and a block permission table for accessing a permission table that describes memory access control information. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Sudia et al. suggest that incorporating a permissions table and revocation information add to the security of the system in order to determine who may or may not gain access to specific resources at the time the user is attempting to do so in par. 237 and par. 245.

Also not explicitly disclosed is checking the integrity of the revocation list and checking the integrity of the block permission table. However, Sudia et al. teach that it is important to check the integrity of the information in the tables that ultimately allow users' access to resources in order to ensure that the permissions/revocation list is being enforced in such a way that a user exceeds their permissions/resources that they should be able to access (par. 219, par. 237, and par. 244-245). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hazard et al. to have an integrity unit in order to ensure the integrity of the revocation list and block permission table. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Sudia et al. suggest that the

permissions and revocation information may be included in the hashed value in order to ensure the validity of the data and that the data has not been improperly modified in par. 219, par. 237, and par. 244-245.

V. Claims 6, 13, 22, and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hazard, United States Patent No. 6,658,566 and Sudia et al., United States Pub. No. 2005/0114666 as applied to claims 1, 8, 17, and 24 above, and further in view of Dilkie et al., United States Patent No. 6,341,164.

As per claims 6 and 22:

Hazard and Sudia et al. substantially teach an information recording device and method, as applied to claims 1 and 17 above. Not explicitly disclosed is the information recording device wherein, in said cryptosystem unit, the encryption processing for the first sector to the M-th sector is executed as triple-DES encryption processing using at least two different encryption keys for each of the sectors. However, Dilkie et al. teaches the use of a triple-DES encryption processing (col. 2, lines 48-54). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the device/method disclosed in Hazard to use triple-DES for the encryption processing. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Dilkie et al. in col. 2, lines 48-54.

As per claims 13 and 29:

Hazard and Sudia et al. substantially teach an information playback device and method, as applied to claims 8 and 24 above. Not explicitly disclosed is the information

Art Unit: 2137

playback device wherein, in said cryptosystem unit, the decryption processing for the first sector to the M-th sector is executed as triple-DES decryption processing using at least two different decryption keys for each of the sectors. However, Dilkie et al. teaches the use of a triple-DES decryption processing (col. 2, lines 48-54). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the device/method disclosed in Hazard to use triple-DES for the decryption processing. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Dilkie et al. in col. 2, lines 48-54.

(10) Response to Argument

Regarding Claims 1, 8, 15, 17, 24, 31, and 32, 35 USC 103(a) Rejections:

Appellant argues Hazard fails to teach/suggest "us[ing] a different encryption key for each sector from the first sector to the M-th sector" or "us[ing] a different decryption key for each sector from the first sector to the M-th sector." Examiner respectfully disagrees. Hazard teaches the use of plural keys for encryption and decryption, where each key is associated with one of the number of items of sensitive information: "*The invention uses **several temporary encrypting protection key CP1,...CPi,...CPn and several associated temporary decrypting protection keys CPd1,...CPdi,...CPdn. Depending on the types of encryption algorithm used, the temporary decrypting***

protection keys may be identical to the temporary encrypting protection keys or different from them” in col. 4, lines 32-38. Hazard further teaches, that these pieces of sensitive information are stored once they have been encrypted using one of the plurality of keys, thereby associating one key per block of sensitive information: “*The table of FIG. 3 includes, in a first column, references to a number m of items of sensitive information IS1, IS2, ... IS(j-1), ISj,...ISm, each of which is stored in the security module in encrypted form using an encryption algorithm and a temporary protection key chosen from among those in the table of FIG. 2. A second column in the table defines the number of the temporary protection key used for each item of sensitive information*” in col. 5, lines 15-22. Finally, the Examiner has given the term “sector” its broadest reasonable interpretation in accordance with MPEP 2111. Hence, the Examiner has interpreted the term to mean a portion of a larger storage block. For the reasons stated above, Examiner believes that Hazard teaches the limitations of using a different encryption/decryption key for each sector from the first sector to the M-th sector.

Appellant further argues that Sudia fails to suggest a “revocation list having revocation information regarding revoked media or content.” Appellant further argues “Sudia discloses privileges and authorizations that are granted to and revoked from a user. The privileges and authorization are not granted to an revoked from media or content.” Examiner respectfully disagrees. First, Examiner would like to point out that the phrase “regarding revoked media or content” is broad and is therefore broadly interpreted according to MPEP 2111. Since the claim language only requires that the

revocation list contains revocation information regarding revoked media or content, **the scope of the claim only requires that the list has information associated with the media or content that has been revoked, whether from one user or from a plurality of users.** Now, in reference to the argued limitation, Sudia teaches a revocation list of information regarding media or content revoked from various users:

"As a matter of pre-arrangement between the recipient/verifier (RV) and the Freshness Service (FS), the FS will, upon receipt of notification of revocation or suspension of a certificate or signature that was recently checked by the RV, either (a) directly push a notice of the revocation to the RV, notify the RV to come and pickup the notice at some given location of the network, or else merely place the notice at some location where the RV will periodically (such as daily) come and pick up any such notices that may have been placed there" in paragraph 209.

Sudia teaches that these revoked privileges are associated with content that the user may no longer access based on the revocation, hence revocation information regarding revoked content: ***"When the user wishes to logon, resume, or continue a session (beyond an agreed maximum duration), the server will request a new proof of non-revocation one or more of the user's privileges, from a Freshness Server, verify it against the THV and cached PFI values stored in its client association record, and resume or refuse (or cancel) the client's access to the content governed by a given privilege, based on the verification results"*** in paragraph 362. Sudia suggests that making use of revocation lists is highly important in order to determine whether or not the user attempting to gain access to specific content is authorized to do so, as well

as to only allow authorized users access: "***First, an organization creates a table or list of possible authorizations for a given user. As shown under the prior art, these strings or list entries can be authorizations, accreditations, restrictions, contractual terms and conditions, references to external variables, filters containing some combination of the foregoing, and so on. This list can be quite long, encompassing every possible privilege string, or it may comprise a subset of the potential privileges the certificate subject is deemed likely to ever need***" in paragraph 237. Thus, Sudia suggests the use of revocation list having revocation information regarding revoked media or content.

Appellant further argues that Hazard and Sudia fail to disclose a "block permission table for accessing a permission table that describes memory access control information." Appellant further argues "The block permission table does not 'lead[s] to various user rights,' as asserted by the Examiner. (Id.) Instead, it accesses a 'permission table that describes memory access control information.' For example, for each block unit of the memory, the block permission table specifies the type of processing permitted, such as 'a block that can be erased, a block that cannot be erased, a block that can be played back, and a block that cannot be played back'." Examiner would first like to point out that since the language used in these examples are not mentioned in the claims, they are not considered to define the scope of the claims. The claims are read in light of the specification, however specific examples from the specification are not read into the claims. Thus, again as interpreted in accordance with MPEP 2111, the block permission table is interpreted as a table

accessing a permissions table describing memory access control information (as claimed), where memory access control information is interpreted as permissions which allow or disallow access (by various users) to various memory elements containing content. Sudia teaches the use of tables/lists that define which users are authorized to access various contents/resources held in various memory elements/locations based on the specific type of data at hand: ***“First, an organization creates a table or list of possible authorizations for a given user. As shown under the prior art, these strings or list entries can be authorizations, accreditations, restrictions, contractual terms and conditions, references to external variables, filters containing some combination of the foregoing, and so on. This list can be quite long, encompassing every possible privilege string, or it may comprise a subset of the potential privileges the certificate subject is deemed likely to ever need”*** in paragraph 237. Thus, Sudia suggests using a block permission table for accessing a permission table that describes memory access control information.

Finally, Appellant argues that Sudia fails to suggest “checking the integrity of the revocation list and block permission table.” Examiner respectfully disagrees. Sudia suggests a method which allows for maintaining the integrity of the revocation list and block permission table using a terminal hash value (THV) which is maintained for the stored privileges in order to make use of an integrity check value for the privileges so that an unauthorized user does not gain access to contents that he/she is not meant to: ***“When the user wishes to logon, resume, or continue a session (beyond an agreed maximum duration), the server will request a new proof of non-revocation one or***

more of the user's privileges, from a Freshness Server, verify it against the THV and cached PFI values stored in its client association record, and resume or refuse (or cancel) the client's access to the content governed by a given privilege, based on the verification results. Note that a universal system for uniquely numbering THVs and PFIs will be useful to assist the server in ascertaining which prior THV a given PFI value goes with, in situations involving multiple THV's for the same client" in paragraphs 362-363. Sudia suggests that the integrity of the permission table and revocation list must be maintained in a verifiable manner since the privileges are generally publicly known: ***"Each OID and privilege value string is further prefixed with a unique random value, or blocker, similar to an initialization vector (IV), of preferably at least 128 bits, such that without knowing this random value, which we will call the 'key' to the authorization string, it will generally be infeasible for the subscriber/sender to present to the recipient/verifier any verifiable proof that he possesses the authorization conferred by a given string. This is necessary because the table of all possible listed authorizations will generally be known, so their hash values could be reconstructed, and hence the digitally signed root node, of the user could allow a user to claim all privileges in the table. However, by blocking each string with a unique and opaque value, the issuer (which may be an Authorization Authority, or "AA") can allow only the currently valid and permitted authorizations to be presented in a verifiable form to the recipient/verifier"*** in paragraphs 239-240. Therefore, Sudia suggests checking the integrity of the revocation list and block permission table.

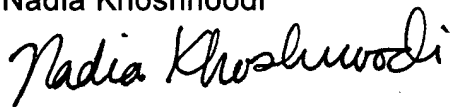
(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Nadia Khoshnoodi

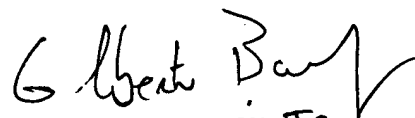


Conferees

Gilberto Barron



Matthew Smithers



GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100